IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MARCUS BAKER, EVA ADAMS, JILLIAN ABBINANTI, ANN BRESNEN, and CAROLE BUCHANAN, individually and on behalf of all others similarly situated, Plaintiffs, - vs - MATCH GROUP, INC. *et al*. Defendants.	Civil Action No.: 3:23-CV-02761-N Hon. David C. Godbey

DEFENDANTS' NOTICE OF SUPPLEMENTAL AUTHORITY

Defendants Match Group, Inc.; Match Group, LLC n/k/a Tinder LLC; Hinge, Inc.; Humor Rainbow, Inc.; People Media, Inc.; and Affinity Apps, LLC respectfully request that the Court consider the new decisions in *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117 (9th Cir. June 17, 2024); *G.T. v. Samsung Electronics America Inc.*, No. 21 CV 4976, 2024 WL 3520026 (N.D. Ill. July 24, 2024); and *Martell v. X Corp.*, No.1:23-cv-05449, 2024 WL 3011353 (N.D. Ill. June 13, 2024) (attached as **Exhibits 1, 2 & 3** respectively) as they relate to Defendants' Motion to Dismiss (ECF # 66 & 67). *Zellmer*, *Samsung*, and *Martell*—each issued after Defendants filed their Reply—confirm that Plaintiffs fail to plausibly allege that Defendants violated the Illinois Biometric Information Privacy Act ("BIPA"), as explained more fully in the Motion to Dismiss and supporting memoranda. While the Court should dismiss this suit because Texas law applies to Plaintiffs' use of Defendants' services, Defendants argue alternatively the Court should dismiss the case for failure to state a claim even if Illinois law applies. These new authorities support this alternative argument.

Description of the New Cases

Zellmer v. Meta Platforms

Zellmer holds as a matter of law that information is a "biometric identifier" or "biometric information" under BIPA only if it is capable of identifying a specific individual. *See* 104 F.4th at 1124-26 (holding that data that merely identifies widespread characteristics such as gender, age, race, hair color, piercings, and generalized facial features cannot constitute biometric information under BIPA).

G.T. v. Samsung

On July 24, the U.S. District Court in *Samsung* applied *Zellmer* and dismissed BIPA claims at the 12(b)(6) stage. The Samsung court ruled that allegations of "face geometry scanning" were insufficient to establish a cognizable BIPA claim. 2024 WL 3520026, at *2, 7. The court held that BIPA "require[s] biometric information to be capable of recognizing an individual's identity, not simply an individual's feature." *Id.* at *8.

Martell v. X Corp.

Martell also dismissed BIPA claims at the 12(b)(6) stage, finding no support for the plaintiff's allegation that the defendant collected biometric information through technology that merely created unique hash algorithms of photographs. 2024 WL3011353, at *2.[1] Although the plaintiff claimed that the "hash" of an image involving a person's face "necessitates creating a scan of that person's facial geometry," these allegations are plainly conclusory and failed to state a claim. *Id*.

[1] Hashing is commonly used to enable rapid data retrieval and verify if corruption occurred during transmission.

The New Authorities Relate to the Motion to Dismiss

As Defendants noted in their opening Motion, Plaintiffs' Amended Complaint pleads at best that Defendants' purported biometric identifiers consist of object recognition and hash algorithms on photographs. *See* ECF # 67 p. 22-23 (arguing that Plaintiffs' allegations concerning the pHash algorithm implausibly alleged facial recognition and explaining that Plaintiffs' allegations concerning Amazon Rekognition technology supported only "object and scene detection"); *see also* ECF # 80 pp. 9-10; ECF # 60 ¶¶ 186, 188, 189-191, 193-197. Significantly, Plaintiffs' leap from hash technology or object recognition to "biometric information" is the same conclusory inference that the Court found deficient in *Martell*. Moreover, *Martell* rejects *Carpenter v. McDonald's Corp.*—a case Plaintiffs heavily relied on—as distinguishable on the facts, just as Defendants argued in their Reply. *See* ECF # 80 p. 8 (distinguishing *Carpenter* on grounds there was no dispute that defendant practiced the patent, which specifically alleged voice recordings were used "to train an AI model to recognize speech"); *Martell*, 2024 WL 3011353, at *3. The *Martell* court held that the plaintiff's factual allegations that an acoustic model was trained to collect and measure acoustic patterns went far beyond the plaintiff's conclusory allegations that the application of hash-technology involved biometric identifiers. *See id*. The same result applies here. As *Martell* confirmed, *Carpenter* is limited to its facts. It does not support the far-reaching result that Defendants' unrelated technology somehow captures biometric information, particularly where Plaintiffs have alleged no specific facts to support it.

Zellmer is also applicable. Plaintiffs' allegations regarding the alternate embodiment in Defendants' matching algorithm fail to describe technology that can be used to specifically identify anyone. This is true even accepting Plaintiffs' allegations that data extracted from photographs can be used to suggest matches or ascertain characteristics like gender or age. *See* ECF # 60 ¶¶ 150-

157; 164-166; 166-173. *Samsung* is equally applicable as an Illinois court confirming *Zellmer's* core holding that biometric technology must recognize an individual's identity, "***not simply an individual's feature***." 2024 WL 3520026, at *8 (emphasis added). Here, as Defendants have maintained, even the patent language relied on by Plaintiffs merely claims that a matching algorithm may be used "to detect ethnicity, hair color, eye color, etc." ECF # 60 ¶ 150 & n.101 (quoting 811 Pat. c. 19 11. 54-58). Thus, like *Zellmer* and *Samsung*, Plaintiffs here fail to allege Defendants collected their biometric information because there are no facts to suggest Defendants' matching algorithm, purported face scanning, or voice note technologies could identify any specific individual.

Dated: August 2, 2024

Respectfully submitted,

DLA PIPER LLP (US)

/s/ *Robert M. Hoffman*
Rob Hoffman (Bar No. 09788200)
rob.hoffman@us.dlapiper.com
John Canoni (Bar No. 24117335)
john.canoni@us.dlapiper.com
1900 N. Pearl Street, Suite 2200
Dallas, Texas 75201
Telephone: (214) 743-4500
Facsimile: (214) 743-4545

BLANK ROME LLP

Daniel R. Saeedi
(*admitted pro hac vice*)
daniel.saeedi@blankrome.com
Rachel L. Schaller
(*admitted pro hac vice*)
rachel.schaller@blankrome.com
444 West Lake Street, Suite 1650
Chicago, Illinois 60606
Telephone: (312) 776-2517
Facsimile: (312) 276-2601

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Stephen A. Broome
(*admitted pro hac vice*)
stephenbroome@quinnemanuel.com
51 Madison Avenue, 22nd Floor
New York, New York 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Counsel for Defendants

EXHIBIT 1

104 F.4th 1117
United States Court of Appeals, Ninth Circuit.

Clayton P. ZELLMER, on behalf of himself and all others similarly situated, Plaintiff-Appellant,

v.

META PLATFORMS, INC., Defendant-Appellee.

No. 22-16925

|

Submitted February 7, 2024 San Francisco, California

|

Filed June 17, 2024

Synopsis

Background: Non-user of social media platform brought putative class action against platform alleging violations of the Illinois Biometric Information Privacy Act (BIPA). The United States District Court for the Northern District of California, James Donato, J., 2022 WL 976981, granted in part and denied in part platform's motion for summary judgment, and then dismissed for lack of standing, 2022 WL 16924098. Non-user appealed.

Holdings: The Court of Appeals, R. Nelson, Circuit Judge, held that:

[1] BIPA protected platform users and non-users alike;

[2] platform's face signature feature was not a "biometric identifier" covered by BIPA; and

[3] non-user lacked standing to pursue claim platform violated BIPA by not making publicly available a policy identifying retention schedule for destroying biometric identifiers or biometric information it had collected.

Affirmed.

Procedural Posture(s): On Appeal; Motion for Summary Judgment; Motion to Dismiss for Lack of Standing.

West Headnotes (21)

[1] **Federal Courts** Summary judgment

Court of Appeals reviews a summary judgment ruling de novo.

[2] **Federal Courts** Summary judgment

In reviewing a summary judgment ruling, the Court of Appeals reviews the facts in the light most favorable to the non-moving party.

[3] **Summary Judgment** Burden of Proof

On motion for summary judgment, the nonmoving party may not rest upon mere allegations or denials of his pleading, but must set forth specific facts showing that there is a genuine issue for trial. Fed. R. Civ. P. 56(a).

[4] **Summary Judgment** Viability of Claim or Defense

Summary Judgment Scintilla of evidence; minimal amount

Mere existence of a scintilla of evidence in support of the plaintiff's position will be insufficient to avoid summary judgment; there must be evidence on which the jury could reasonably find for the plaintiff. Fed. R. Civ. P. 56(a).

[5] **Summary Judgment** Preponderance of evidence

The judge's inquiry on motion for summary judgment unavoidably asks whether reasonable jurors could find by a preponderance of the evidence that the plaintiff is entitled to a verdict. Fed. R. Civ. P. 56(a).

[6] **Federal Courts** Standing

Court of Appeals reviews a grant of a motion to dismiss for lack of standing de novo.

[7] **Federal Courts** Dismissal for lack of jurisdiction

In reviewing a ruling on a motion to dismiss for lack of standing, Court of Appeals accepts the allegations in the complaint as true.

[8] **Statutes** Language and intent, will, purpose, or policy

In Illinois, courts regard the language of the statute as the best indication of legislative intent.

[9] **Statutes** Giving effect to statute or language; construction as written

Statutes Relation to plain, literal, or clear meaning; ambiguity

Under Illinois law, when the language of the statute is clear, it must be applied as written without resort to aids or tools of interpretation, even though the consequences may be harsh, unjust, absurd or unwise.

[10] **Antitrust and Trade Regulation** Privacy

The Illinois Biometric Information Privacy Act (BIPA) protected social media platform users and non-users alike, for purposes of non-user's claims alleging that platform violated BIPA when it collected or captured his biometric identifiers when it created a face signature from uploaded photographs; BIPA's language, that no private entity was allowed to collect, capture, purchase, receive through trade, or otherwise obtain a "person's or a customer's" biometric data without his consent showed that statute applied to everyone whose biometric identifiers or information was held by platform, regardless of any preexisting relationship with platform. 740 Ill. Comp. Stat. Ann. 14/15(b).

[11] **Antitrust and Trade Regulation** Privacy

Under the Illinois Biometric Information Privacy Act (BIPA), which prevents private entities from collecting or obtaining a person's or customer's biometric identifier or biometric information, the term "identifier" means one that identifies a person. 740 Ill. Comp. Stat. Ann. 14/10, 14/15(b).

1 Case that cites this headnote

[12] **Statutes** Associated terms and provisions; noscitur a sociis

Generally, the words in a list provided by statute should be given similar meanings.

[13] **Statutes** Construction based on multiple factors

A statute's language, structure, subject matter, context, and history are all factors that typically help courts determine a statute's objectives and thereby illuminate its text.

[14] **Statutes** Statute as a Whole; Relation of Parts to Whole and to One Another

In Illinois, courts must read a statute as a whole and consider all relevant parts.

[15] **Antitrust and Trade Regulation** Privacy

Social media platform's face signatures feature which allowed users to connect to friends through photographs uploaded to the platform was not a "biometric identifier" covered by the Illinois Biometric Information Privacy Act (BIPA), because it could not be used to identify any individual person; platform's face signature was merely a string of numbers that represented a particular image of a face and did not reveal any geometric information about the face detected in the image, nor did they correspond to facial features like the eyes or nose, or distances between them, and faces of non-users that appeared in photographs were anonymous to platform. 740 Ill. Comp. Stat. Ann. 14/15(b).

1 Case that cites this headnote

[16] **Federal Civil Procedure** In general; injury or interest

Federal Courts Case or Controversy Requirement

Article III's case or controversy requirement limits federal courts' subject matter jurisdiction by requiring, inter alia, that plaintiffs have standing. U.S. Const. art. 3, § 2, cl. 1.

[17] **Federal Civil Procedure** In general; injury or interest

Federal Civil Procedure Causation; redressability

A plaintiff must demonstrate standing by establishing the irreducible constitutional minimum of (1) an injury in fact (2) fairly traceable to the defendant's challenged conduct (3) that is likely to be redressed by a favorable decision. U.S. Const. art. 3, § 2, cl. 1.

[18] **Federal Civil Procedure** In general; injury or interest

A plaintiff shows injury in fact, as required for standing, if he has suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical. U.S. Const. art. 3, § 2, cl. 1.

[19] **Antitrust and Trade Regulation** Privacy

A private entity's duty to disclose a data retention schedule and guidelines for permanently destroying collected biometric identifiers and information under the Illinois Biometric Information Privacy Act (BIPA) is owed to the public generally, not to particular persons whose biometric information the entity collects. 740 Ill. Comp. Stat. Ann. 14/15(a).

1 Case that cites this headnote

[20] **Courts** Conclusiveness of decisions of Court of Appeals within its circuit

Federal courts' custom on questions of state law ordinarily is to defer to the interpretation of the Court of Appeals for the circuit in which the state is located.

[21] **Antitrust and Trade Regulation** Private entities or individuals

Federal Civil Procedure Particular Classes Represented

Non-user of social media platform lacked standing to pursue claim in putative class action that platform violated the Illinois Biometric Information Privacy Act (BIPA) by not having written, publicly available policies identifying its retention schedules for permanently destroying any biometric identifiers or information on non-users like himself in its possession, where non-user did not show that his BIPA-protected data was ever in platform's possession or that he or any putative class members had been harmed in a particularized way different from the public generally. U.S. Const. art. 3, § 2, cl. 1; 740 Ill. Comp. Stat. Ann. 14/15(b).

***1119** Appeal from the United States District Court for the Northern District of California, James Donato, District Judge, Presiding, D.C. No. 3:18-cv-01880-JD

Attorneys and Law Firms

John Carey (argued), Carey Rodriguez LLP, Miami, Florida; David P. Milian, The Milian Legal Group, Miami, Florida; Albert Y. Chang, Bottini & Bottini Inc., La Jolla, California; for Plaintiff-Appellant.

Lauren R. Goldman (argued), Michael Brandon, and Lefteri J. Christos, Gibson Dunn & Crutcher LLP, New York, New York; Michael G. Rhodes and Whitty Somvichian, Cooley LLP, San Francisco, California; John Nadolenco, Mayer Brown LLP, Los Angeles, California; for Defendant-Appellee.

Roman Martinez and Jeremy L. Brown, Latham & Watkins LLP, Washington, D.C.; Gary Feinerman, Latham & Watkins

LLP, Chicago, Illinois; for Amicus Curiae, Security Industry Association.

Before: Ryan D. Nelson, Danielle J. Forrest, and Gabriel P. Sanchez, Circuit Judges.

OPINION

R. NELSON, Circuit Judge:

Clayton Zellmer has never used Facebook. He sued Facebook—now Meta Platforms—for alleged violations of the Illinois Biometrics Information Privacy Act after his friends uploaded photographs of him to Facebook. He alleged that Facebook collected or captured his biometric identifiers when it created what Facebook calls a "face signature" from those uploaded photos. ***1120** The district court granted summary judgment to Facebook on that claim. Zellmer also alleged that Facebook failed to publish a written policy establishing its retention schedule for collected biometric data. The district court dismissed that claim for lack of standing. We have jurisdiction under 28 U.S.C. § 1291, and we affirm.

I

A

Under the Illinois Biometrics Information Privacy Act (BIPA), a private entity can "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" only if it:

- Informs the subject or her representative in writing of the collection or storage of her biometric identifier or information;
- Informs the subject or her representative in writing of "the specific purpose and length of term" for their use; and
- Receives written authorization to do so from the subject or her representative.

740 ILL. COMP. STAT. 14/15(b) (Section 15(b)). A "biometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id.* 14/10. As potentially relevant, biometric identifiers do not include photographs. *Id.* For its part, "biometric information" is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual" and "does not include information derived from items or procedures excluded under the definition of biometric identifiers." *Id.*

Any company that possesses biometric identifiers or information must "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information." *Id.* 14/15(a) (Section 15(a)). The required policy must clarify that any collected biometric identifier or information will be deleted "when the initial purpose" for the collection "has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." *Id.* To ensure compliance, BIPA grants a "right of action" against an "offending party" to anyone aggrieved by a violation of its terms. *Id.* 14/20.

B

"In 2010, Facebook launched a feature called Tag Suggestions." *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1268 (9th Cir. 2019). If a user enables Tag Suggestions, Facebook "analyze[s] whether the user's Facebook friends are in photos uploaded by that user." *Id.* If there is a match, then Facebook suggests that the user "tag" his friend. *Id.* The Tag Suggestions feature proceeds in four steps.

The first step is the Detection Stage. Facebook analyzes the photo to determine whether it includes any human faces. If Facebook detects a human face, it produces a cropped image of the face. Nothing more is done at this stage.

The next step is the Alignment Stage. Facebook takes any cropped image of a face and standardizes it by centering it, bringing it forward, and scaling it. Facebook is not always successful at standardizing a photo's detected faces. But if alignment is successful, then Facebook moves to the third step.

That step—which is the focus of this appeal—is the Representation Stage. Facebook tries to create what it calls a "face signature." A face signature is a string of numbers that represents a particular image of a face. Face signatures do

not—and cannot—reveal information about a face's ***1121** geometric information. And they neither reveal facial features nor the distances between them. They are simply numbers—an abstract, numerical representation of the aligned face crop created in previous stages. No one—not even Facebook—can reverse-engineer the numbers comprising a given face signature to derive information about a person. And even if the reverse-engineering of a face signature were technically possible, face signatures exist for only a tiny fraction of a second—they are neither saved nor stored after the final stage of the Tag Suggestions process.

The final step is the Classification Stage, which occurs immediately after a face signature is created. At this point, Facebook compares the face signature to what it calls face templates, which are only created for Facebook users. Facebook does not run the new face signature against every face template it has. Instead, it compares the face signature with the face templates of users who have both enabled face recognition and are connected to the user who uploaded the photo from which Facebook created the face signature. Regardless of whether the comparison yields a match, the face signature is immediately deleted.

C

After Zellmer's friends uploaded photos of him to Facebook, he sued Facebook (now Meta, which we use interchangeably) alleging violations of Sections 15(a) and 15(b) of BIPA by collecting, using, and storing biometric identifiers from photos without first obtaining written consent and establishing a public retention schedule.

After discovery, the district court granted summary judgment to Meta on Zellmer's Section 15(b) claim, finding that this statutory section did not protect the privacy interests of non-users. *Zellmer v. Facebook, Inc.*, No. 3:18-CV-01880-JD, 2022 WL 976981, at *5 (N.D. Cal. Mar. 31, 2022). In the district court's view, "it would be patently unreasonable to construe BIPA to mean that Facebook was required to provide notice to, and obtain consent from, non-users who were for all practical purposes total strangers to Facebook, and with whom Facebook had no relationship whatsoever." *Id.* at *3. The court considered this construction of Section 15(b) "untenable" because it deviated from the Illinois legislature's intent and would lead to absurd results, such as putting Meta in the "impossible position" of "obtain[ing] consent from every stranger whose face happened to be caught on camera." *Id.* at *3–5. And that requirement would require Meta to abandon Tag Suggestions everywhere to avoid violating the law in Illinois. Such a result, the court explained, was impossible to square with the Supreme Court of Illinois's conclusion that BIPA "should not impose extraordinary burdens on businesses." *Id.* at *5; *accord* *id.* at *3 (quoting *Rosenbach v. Six Flags Ent. Corp.*, 432 Ill.Dec. 654, 129 N.E.3d 1197, 1207 (Ill. 2019)).

The district court denied Meta summary judgment on the Section 15(a) claim, finding that there is a factual dispute to be resolved at trial. *Id.* at *5. A few months later, the district court addressed Zellmer's standing to bring a Section 15(a) claim. *Zellmer v. Facebook, Inc.*, No. 3:18-CV-01880-JD, 2022 WL 16924098 (N.D. Cal. Nov. 14, 2022). It held that Zellmer lacked Article III standing because he did not suffer a particularized injury and dismissed the Section 15(a) claim. *Id.* at *2–4.

II

[1] **[2]** **[3]** **[4]** **[5]** We review "a summary judgment ruling de novo." *Guzman v. Polaris Indus. Inc.*, 49 F.4th 1308, 1311 (9th Cir. 2022). We review the facts in the light most favorable to the non-moving party. *Scott v. Harris*, 550 U.S. 372, 380, 127 S.Ct. 1769, 167 L.Ed.2d 686 (2007). "[I]f ***1122** the nonmoving party contests summary judgment, the alleged factual dispute must be both genuine and material to the nonmoving party's claims." *Momox-Caselis v. Donohue*, 987 F.3d 835, 841 (9th Cir. 2021). But the nonmoving party "may not rest upon mere allegations or denials of his pleading, but must set forth specific facts showing that there is a genuine issue for trial." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 256, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). "The mere existence of a scintilla of evidence in support of the plaintiff's position will be insufficient; there must be evidence on which the jury could reasonably find for the plaintiff." *Id.* at 252, 106 S.Ct. 2505. "The judge's inquiry, therefore, unavoidably asks whether reasonable jurors could find by a preponderance of the evidence that the plaintiff is entitled to a verdict." *Id.* We "may affirm on any ground supported by the record." *Maner v. Dignity Health*, 9 F.4th 1114, 1119 (9th Cir. 2021).

[6] **[7]** We likewise review a grant of a motion to dismiss for lack of standing de novo. *Wakefield v. ViSalus, Inc.*, 51 F.4th 1109, 1117 (9th Cir. 2022). In reviewing a ruling on a motion to dismiss, we accept the allegations in the complaint as true. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009).

III

A

We begin by rejecting the grounds on which the district court granted summary judgment to Meta. As we explained above, *see supra* Part I.C, the district court's decision turned on the practical impossibility of Meta's complying with BIPA if it had to obtain consent from everyone whose photo was uploaded to Facebook before it could employ Tag Suggestions. Because the plain text applies to everyone whose biometric identifiers or information is held by Facebook, this conclusion was wrong.

[8] **[9]** To explain why, we look to the statutory text. *See Tanzin v. Tanvir*, 592 U.S. 43, 46, 141 S.Ct. 486, 208 L.Ed.2d 295 (2020). Since BIPA is an Illinois statute, we interpret it consistent with how it would be interpreted by Illinois courts. In Illinois, courts "regard the language of the statute as the best indication of legislative intent." *U.S. Fire Ins. Co. v. Barker Car Rental*, 132 F.3d 1153, 1156 (7th Cir. 1997) (citing *Abrahamson v. Ill. Dep't of Pro. Regul.*, 153 Ill.2d 76, 180 Ill.Dec. 34, 606 N.E.2d 1111, 1118 (1992)). "[W]hen the language of the statute is clear, it must be applied as written without resort to aids or tools of interpretation," *DeLuna v. Burciaga*, 223 Ill.2d 49, 306 Ill.Dec. 136, 857 N.E.2d 229, 236 (2006), "even though the consequences may be harsh, unjust, absurd or unwise," *Cothron v. White Castle Sys., Inc.*, 466 Ill.Dec. 85, 216 N.E.3d 918, 928 (Ill. 2023) (cleaned up).

[10] Here, Section 15(b)'s language is clear: "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a *person's or a customer's*" biometric data without his consent. 740 ILL. COMP. STAT. 14/15(b) (emphasis added). By delineating between persons and customers, BIPA shows that non-users are protected, regardless of any preexisting relationship with the party alleged to have violated BIPA. The only relevant question is whether Meta has collected or captured Zellmer's biometric data without his consent. If it has, then it has violated BIPA—even if Meta lacks privity with Zellmer. Contrary to the district court's conclusion, even if it were "patently unreasonable" to provide a cause of action to "total strangers to Facebook, and with whom Facebook had no relationship," BIPA's plain terms do just that. *Zellmer*, 2022 WL 976981, at *3.

B

***1123** Rejecting the district court's reasons for granting summary judgment, however, does not resolve this case. Having determined that BIPA protects users and non-users alike, we turn to whether there is a material dispute of fact as to whether Meta violated BIPA's plain terms. On the record before us, there is no dispute that Facebook made a face signature of Zellmer from photos that his friends uploaded. Our question, then, is whether a face signature is either a biometric identifier or biometric information for BIPA purposes. Guided by "the statutory text," *Tanzin*, 592 U.S. at 46, 141 S.Ct. 486, we conclude that it is neither.

1

Meta argues that BIPA applies only to biometric identifiers and information that can identify a person. Section 15(b) of BIPA protects not only "biometric information" that identifies an individual, but also "biometric identifiers" themselves. These "identifiers" are defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILL. COMP. STAT. 14/10. In other words, if either form of biometric data cannot identify an individual, it is not an identifier and thus not covered by BIPA. As evidence, Meta cites not only the dictionary definition of "identifiers," [1] but also case law showing that biometric identifiers must be a feature that can identify a person. Zellmer responds that, while biometric information requires the ability to "identify an individual," biometric identifiers have no such explicit requirement. We join the other courts to have considered this issue and reject Zellmer's argument.

Zellmer would write the term "identifier" out of BIPA. Under his reading, every "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" is a biometric identifier and therefore within BIPA's reach. 740 ILL. COMP. STAT. 14/10. But this reading conflates necessary and sufficient conditions. The defined term imposes on the ordinary meaning of "biometric identifiers" a set of necessary conditions. Something that falls outside the defined statutory definition (such as a photograph) can be a biometric identifier under the term's plain meaning, but not be covered by BIPA's statutory definition. On the other hand, something can otherwise fall within BIPA's specific list of potential "biometric identifiers," but still not be covered if it cannot identify. For example, scans of face geometry fall within BIPA's list, but are not covered by BIPA if they cannot identify a person.

To understand why, we look to the Supreme Court's explanation that "[i]n settling on a fair reading of a statute, it is not unusual to consider the ordinary meaning of a defined term, particularly when there is dissonance between that ordinary meaning and the reach of the definition." *Bond v. United States*, 572 U.S. 844, 861, 134 S.Ct. 2077, 189 L.Ed.2d 1 (2014). In *Bond*, the Court interpreted Congress's defined term "chemical weapon" against the backdrop of its ordinary meaning. *Id.* In so doing, the Court concluded that the defendant did not engage in chemical warfare by using a chemical weapon when she "spread [common] chemicals on her car door, mailbox, and door knob" to cause her husband's mistress to "develop an uncomfortable rash." *Id.* at 852, 134 S.Ct. 2077. Even though the term "chemical weapon" ***1124** included "toxic chemicals" such as those used by the defendant, *id.* at 850, 134 S.Ct. 2077, "the global need to prevent chemical warfare does not require the Federal Government to reach into the kitchen cupboard, or to treat a local assault with a chemical irritant as the deployment of a chemical weapon," *id.* at 866, 134 S.Ct. 2077.

The Supreme Court frequently considers the ordinary meaning of a statutorily defined term. In *Sackett v. Environmental Protection Agency*, the Court "refused to read 'navigable' out" of the Clean Water Act, even though it recognized that the statutorily defined term "extends to more than traditional navigable waters." 598 U.S. 651, 672, 143 S.Ct. 1322, 215 L.Ed.2d 579 (2023). And the Court refused to interpret "violent felony"—statutorily defined as a crime that uses "physical force"—to require less than "force capable of causing physical pain or injury." *Johnson v. United States*, 559 U.S. 133, 140, 130 S.Ct. 1265, 176 L.Ed.2d 1 (2010). And it did so despite recognizing that "physical force" was broad enough to "have meant *any* force, however slight." *Bond*, 572 U.S. at 862, 134 S.Ct. 2077 (discussing *Johnson*).

[11] Applying that interpretive principle here, we conclude that the ordinary meaning of "identifier"—since it has an -er suffix—is "one that identifies." We are persuaded that the term's ordinary meaning informs its statutory meaning. As in *Bond*, where the statute's reach was limited by the term's ordinary meaning despite a statutory definition, applying the ordinary meaning of "identifier" would ensure that Meta is not forced to abandon key services that it offers its customers or risk perpetual liability. As Zellmer recognizes, these are the only two paths forward under his reading of the statute.

[12] The list of "biometric identifiers" that the statute lists compels the same conclusion. Each of the listed items—retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry—are unique to a person. Each can thus be used to identify a person in the proper context. Generally, the words in a list should be given similar meanings. *Aguayo v. U.S. Bank*, 653 F.3d 912, 927 (9th Cir. 2011). The unifying theme behind each term here is that each identifies a person.

[13] **[14]** Further, as Meta and amicus explain, BIPA's context supports a conclusion that "biometric identifiers" must identify. "[T]he statute's language, structure, subject matter, context, and history" are all "factors that typically help courts determine a statute's objectives and thereby illuminate its text." *Almendarez-Torres v. United States*, 523 U.S. 224, 228, 118 S.Ct. 1219, 140 L.Ed.2d 350 (1998). That principle applies with no less force in Illinois, where courts must "read[ ] the statute as a whole and consider[ ] all relevant parts." *Sylvester v. Indus. Comm'n*, 197 Ill.2d 225, 258 Ill.Dec. 548, 756 N.E.2d 822, 827 (2001). Other statutory definitions thus illuminate BIPA's reach.

Take "biometric information." As Zellmer recognizes, unlike "biometric identifier," "biometric information" applies only to information "used to identify an individual." 740 ILL. COMP. STAT. 14/10. And Section 15(e) requires both identifiers and information to be afforded the protections

given to "other confidential and sensitive information," *id.* 14/15(e)(2), defined as "personal information that can be used to *uniquely identify*" a person, *id.* 14/10 (emphasis added). Both terms thus turn on the ability to identify an individual. Reading the statute "as a whole," it makes sense to impose a similar requirement on "biometric identifier," particularly because the ability to identify did not need to be spelled out in that term—it was readily apparent from the use of "identifier." *Sylvester*, 258 Ill.Dec. 548, 756 N.E.2d at 827.

***1125** Other courts have interpreted BIPA and reached the same conclusion. One such case, *Hazlitt v. Apple*, 500 F. Supp. 3d 738 (S.D. Ill. 2020), *judgment vacated on other grounds sub nom. In re Apple Inc.*, No. 20-8033, 2021 WL 2451296 (7th Cir. Jan. 22, 2021), is particularly persuasive since it was decided in Illinois on an issue of Illinois law. The *Hazlitt* plaintiffs alleged that Apple analyzed photographs saved to its Photo app to "specifically identify the Apple device user" and allowed users to tag "names for each of the faces detected in the People album" on the device. *Id.* at 742. In its motion to dismiss, Apple argued that "these facial scans cannot qualify as biometric identifiers because Apple *does not* use the scans to actually identify a person." *Id.* at 749 (emphasis added). The *Hazlitt* court rejected Apple's interpretation as too narrow because "[t]he word 'identifier' modifies the word 'biometric' to signal that the types of data listed *could* be used to identify a person." *Id.* (emphasis in original). *Hazlitt* thus recognized that, even if a company *does not* use face scans to identify a person, BIPA applies if it *could*. Given that understanding, the *Hazlitt* court denied the motion to dismiss because the complaint alleged "that the Photos app applies an algorithm to identify the device user," a fact that the court took "as true, at this stage." *Id.* *Hazlitt* reflects the broad consensus that "biometric identifiers" under BIPA must be able to identify. [2]

2

[15] Meta's argument is different from Apple's in *Hazlitt*. Rather than arguing—like Apple—that Meta *does not* use the information it collected to identify anyone, Meta argues that the undisputed evidence shows that face signatures *cannot* identify non-users. Given our interpretation of "biometric identifiers" and the "biometric information" derived from them, if Meta is correct, then face signatures are not biometric identifiers or information under BIPA. The district court concluded, in a single sentence, that there was a dispute about whether face signatures can identify non-users. *Zellmer*, 2022 WL 976981, at *5. Having independently reviewed the record and the evidence cited by the parties, we conclude, contrary to the district court, that there is no material dispute of fact about whether face signatures can identify a person. *See Maner*, 9 F.4th at 1119. We affirm the grant of summary judgment in Meta's favor on that basis.

To support its claim that face signatures are not biometric identifiers, Meta submitted a declaration from Gary McCoy, a Product Manager at Facebook. He explained that a face signature is merely "a string of numbers that represents a particular image of a face." Those numbers "do not reveal any geometric information about the detected face in the image, nor do they correspond to facial features like the eyes or nose, or distances between them." Instead, a face signature is "an abstract, numerical representation of a face crop that is computed by millions of pixel comparisons performed by the proprietary algorithm that Facebook has developed," which "cannot be reverse-engineered" and is neither "saved [n]or stored." Because the numbers that constitute a face signature cannot be reverse engineered, McCoy explained that "faces of non-users ... that appear in photos are anonymous to Facebook" and that "it is not possible to identify" non-users from ***1126** their face signatures. The creation of face signatures "do[es] not create or store any other data from the detected faces of non-users ... that could be used to recognize or identify them through the use of face recognition."

To dispute the McCoy declaration, Zellmer offers evidence that the face signature can predict a person's age and gender and that Meta turns on what is called the "recognizable indicator," which is "associated with a given face," for face signatures. Finally, he notes that face signatures "include the geometric x and y coordinates within the photo where a person's face appears, thus calculating the dimensions of the person's face."

Neither piece of evidence can carry the weight Zellmer affords it. That a face signature can predict a person's gender limits the pool of potential matches to approximately 50% of the population; this fails to identify anyone. Nor is a person's age—standing alone or together with his or her gender—able to identify a person. Nor is the gender-identification always accurate: Zellmer himself erroneously matched to a

woman from the face signatures that Meta created. As for the recognizable indicator being turned on, this means only that the image can advance to the standardization phase—Meta's process for determining whether it can create a face signature. Put differently, the recognizable indicator allows Meta only to identify that a particular image contains a face. But this does not mean that Meta can, from that face, identify a person. Nor do the coordinates within the photos that can map out the size of a person's face show that Meta can, from those coordinates, identify an unknown person.

These are the three key facts which Zellmer relied on below. And he points to no new evidence in the record on appeal. None of these facts rebuts Meta's showing that a face signature, which is all that was ever created for Zellmer, cannot identify him. Zellmer must identify both the evidence that creates a dispute of fact and the reasons why that evidence creates a dispute. *See* *Anderson*, 477 U.S. at 256, 106 S.Ct. 2505 (nonmoving party "must set forth specific facts showing that there is a genuine issue for trial"). Zellmer has not carried that burden. There is therefore no dispute of fact on this point. And because—on the record before us—face signatures cannot identify, they are not biometric identifiers or biometric information as defined by BIPA.[3] Accordingly, summary judgment to Meta was appropriate.

IV

We also affirm the district court's dismissal of the Section 15(a) claim for lack of standing. Zellmer alleges that Meta lacks written, publicly available policies identifying its retention schedules for permanently destroying any biometric identifiers or information of non-users like him in its possession.

[16] **[17]** **[18]** Article III's "case or controversy" requirement "limits federal courts' subject matter jurisdiction by requiring, inter alia, that plaintiffs have standing." *Chandler v. State Farm Mut. Auto. Ins.*, 598 F.3d 1115, 1121 (9th Cir. 2010). A plaintiff must demonstrate standing by establishing the "irreducible constitutional minimum" of (1) an injury in fact (2) fairly traceable to the defendant's challenged conduct (3) that is likely to be redressed by a favorable decision. ***1127** *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338, 136 S.Ct. 1540, 194 L.Ed.2d 635 (2016) (citation and quotation omitted). A plaintiff shows injury in fact if he has "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.' " *Id.* at 339, 136 S.Ct. 1540 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992)).

[19] **[20]** These well-trodden principles compel our conclusion that Zellmer lacks standing to bring his Section 15(a) claim. Because this claim was resolved on a motion to dismiss, we look to the operative complaint. Zellmer alleges a single sentence about Section 15(a): "Facebook does not publicly provide a retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information of Plaintiff and the Class members." But as the Seventh Circuit has concluded, this is a duty owed not to any particular person, but to the "public generally." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020); *accord* *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1154 (7th Cir. 2020).[4]

[21] Zellmer never explained how he or any of the proposed class members are harmed by violations of this general duty in a "concrete and particularized" way. Nor could he have, given our conclusion that—on the record before us—face signatures are not biometric identifiers or information. As a result, Meta's creation of face signatures does not lead to the "very substantive harm targeted by BIPA." *Patel*, 932 F.3d at 1275. And, as Zellmer concedes, if there is no Section 15(b) violation, he lacks standing to bring a Section 15(a) claim. Because face signatures are neither biometric identifiers nor information, Zellmer is no more harmed by Meta's failure to have a retention schedule or guidelines related to the destruction of biometric identifiers or information than anyone else in Illinois.

Our decision in *Patel* is not to the contrary. There, we held that BIPA established "concrete interests" in privacy, not merely procedural rights. 932 F.3d at 1274. We then considered whether the violations Patel alleged harmed those concrete interests. *Id.* We concluded that they did. In so concluding, we explained that plaintiffs alleged that Facebook created a "face template" of them from uploaded photos, the "very substantive harm targeted by BIPA." *Id.* at 1275. This violation of Section 15(b) was sufficient to confer Article III standing. And because they had alleged a violation of Section 15(b), they could show direct and discrete harm from

the alleged Section 15(a) violation. *See* *id.* at 1275–76. Zellmer has not shown that his BIPA data was ever in Meta's possession or that he has been harmed in a particularized way different from the public generally. Thus, *Patel* does not resolve the allegations here.

V

Meta is entitled to summary judgment on the Section 15(b) claim. And Zellmer ***1128** lacks standing to bring his Section 15(a) claim.

AFFIRMED.

All Citations

104 F.4th 1117, 2024 Daily Journal D.A.R. 5258

Footnotes

1 An "identifier" is "one that identifies," and "identify" means "to ascertain the identity of [something or someone]." *Identifier*, MERRIAM-WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/identifier; *Identify*, MERRIAM-WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/identify.

2 *See* *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017) ("Each specific item on the list, not surprisingly, fits within the meaning of the term 'biometric identifier,' that is, a biology-based set of measurements ('biometric') that *can be used to identify* a person ('identifier')." (emphasis added)); *Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1296 (W.D. Wash. 2021) (same).

3 Given this conclusion, we need not decide whether Meta's creation—and near immediate deletion—of a face signature skirts BIPA's prohibition on "collect[ing], captur[ing], purchas[ing], receiv[ing] through trade, or otherwise obtain[ing]" a biometric identifier. 740 ILL. COMP. STAT. 14/15(b).

4 Meta argues that, because the Seventh Circuit "possesses greater familiarity with" Illinois law, its interpretation of BIPA is afforded greater weight. *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 16, 124 S.Ct. 2301, 159 L.Ed.2d 98 (2004). "Our custom on questions of state law ordinarily is to defer to the interpretation of the Court of Appeals for the Circuit in which the State is located." *Id.* But the "question now before us is whether, for federal-court purposes, ... a person has suffered the kind of injury-in-fact that supports Article III standing." *Bryant*, 958 F.3d at 619. As with all standing questions, we review the district court de novo—guided, as required, by the Seventh Circuit's interpretation of BIPA.

EXHIBIT 2

2024 WL 3520026
Only the Westlaw citation is currently available.
United States District Court, N.D. Illinois, Eastern Division.

G.T., et al., Plaintiffs,
v.
SAMSUNG ELECTRONICS AMERICA INC., et al., Defendants.

No. 21 CV 4976
|
Signed July 24, 2024

Attorneys and Law Firms

Gregg M. Barbakoff, Keith James Keogh, Theodore Herbert Kuyper, Keogh Law, Ltd., Chicago, IL, for Plaintiff G.T.

Gregg M. Barbakoff, Keogh Law, Ltd, Chicago, IL, for Plaintiff Shimera Jones.

Gregg M. Barbakoff, Keogh Law, Ltd., Chicago, IL, for Plaintiffs LeRoy Jacobs, Richard Maday, Mark Heil, Balarie Cosby-Steele, Sherie Harris, John DeMatteo, Allison Thurman.

Ashley Marie Pavel, O'Melveny & Myers LLP, Newport Beach, CA, Emily Elizabeth Dory, Mark Howard Boyle, Mason William Kienzle, Donohue Brown Mathewson & Smyth LLC, Chicago, IL, Matthew D. Powers, Pro Hac Vice, Randall W. Edwards, Pro Hac Vice, O'Melveny & Myers LLP, San Francisco, CA, for Defendants.

MEMORANDUM OPINION AND ORDER

Lindsay C. Jenkins, United States District Judge

***1** Defendants Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. (collectively, "Samsung") have moved to dismiss the consolidated amended class complaint filed by several Plaintiffs [1] who allege facial recognition technology in Samsung's Gallery photo application violates Illinois's Biometric Information Privacy Act ("BIPA"). For the reasons stated herein, the motion is granted.

I. Background

The Court takes Plaintiffs' well-pleaded factual allegations as true for purposes of ruling on the motion to dismiss. *See Smith v. First Hosp. Lab'ys, Inc.*, 77 F.4th 603, 607 (7th Cir. 2023). Samsung manufactures various smartphones and tablets ("Devices"), and Plaintiffs are all Illinois residents who used Samsung Devices. All Devices come pre-installed with the Gallery application (the "App"), which Samsung designs and owns. [Dkt. 50 ¶¶ 2-3, 12; *see also id.* at 17-35.] [2]

The App allows users to "save, organize, edit, share and store" their videos and photographs, and everything captured by the Device's camera is saved on the App. [*Id.* ¶ 3.] But that is not all. Plaintiffs allege that the App automatically takes a series of actions when an image is created. First, Samsung's "proprietary facial recognition technology" scans images to search for faces. If the App detects a face, it analyzes the face's "unique facial geometry." [3] Based on this analysis, the App creates a unique digital representation of the face, called a "face template." [*Id.* ¶¶ 4-6; 52-54.]

Once a face template is created, the App organizes photographs based on images with similar face templates. The App does this through "face clustering", a process by which the App extracts key facial features from the face template and converts that information into numerical "vectors" based on the facial feature. The App compares the vectors in a new image to the previous images on the Device and will group together images that are sufficiently analogous. The result is pictures with a certain individual's face are "stacked" together on the App. [*Id.* ¶¶ 55-56.]

Plaintiffs allege this repository of digital face templates and corresponding vectors (collectively, the "Data") exists "at least" on the Samsung device itself. [*Id.* ¶ 54.] Plaintiffs do not affirmatively allege the Data is sent to any centralized Samsung repository or database, or that Samsung can access the Data on individual Devices.

Plaintiffs contend that through the process of generating the Data, Samsung is collecting the biometrics of all individuals whose faces appear in pictures on its Devices in violation of BIPA. Plaintiffs also allege that they are powerless to protect their biometric information because Samsung does not inform its users of these functions, nor does Samsung permit its users to disable them. According to Plaintiffs, it is an intractable part of the App. And because Samsung designs and installs the App, it has full control over what data is collected, as well as all components of the Data itself, including where and how it is stored. [*Id.* ¶¶ 57-63.] Accordingly, Plaintiffs

sued Samsung alleging it has failed to abide by two BIPA provisions related to steps private entities must follow when they possess biometric data. [Dkt. 50]; 740 ILCS 14/15(a)(b). Samsung now moves to dismiss.

II. Legal Standard

***2** At the motion to dismiss stage, the Court takes well-pleaded factual allegations as true and draws reasonable inferences in favor of the plaintiff. *Choice v. Kohn L. Firm, S.C.*, 77 F.4th 636, 638 (7th Cir. 2023); *Reardon v. Danley*, 74 F.4th 825, 826-27 (7th Cir. 2023). "To survive a motion to dismiss under Rule 12(b)(6), plaintiff's complaint must allege facts which, when taken as true, plausibly suggest that the plaintiff has a right to relief, raising that possibility above a speculative level." *Cochran v. Ill. State Toll Highway Auth.*, 828 F.3d 597, 599 (7th Cir. 2016) (cleaned up). This occurs when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Garrard v. Rust-Oleum Corp.*, 575 F. Supp. 3d 995, 999 (N.D. Ill. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (internal citations omitted)).

III. Analysis

BIPA governs the collection, use, safeguarding, retention, disclosure, and disclosure of biometric data by private entities. The Illinois legislature enacted BIPA to ease public concern regarding "the use of biometrics when such information is tied to finances and other personal information" because biometrics "are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c)-(d).

BIPA defines biometrics in two ways: "biometric identifier" and "biometric information."[4] Biometric identifier "means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry", but excludes items like writing samples and photographs. Biometric information "means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

Under BIPA, private entities that are "in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information." 740 ILCS 14/15(a). In addition, before a private entity "collect[s], capture[s], purchase[s] ... or otherwise obtain[s] a person's" Biometrics, they must inform the person in writing (i) that they are collecting or storing the Biometrics; (ii) why and for how long they are storing the Biometrics; and (iii) receive a written release from the person authorizing the collection. 740 ILCS 14/15(b).

Plaintiffs contend Samsung is in violation of these provisions through the App's use of face geometry scanning, and its creation and storage of Data. Samsung points to two main reasons why Plaintiffs' allegations are insufficient. First, Plaintiffs do not adequately allege that Samsung "possesses", "collects", or "otherwise obtains" Biometrics because Plaintiffs do not allege the Data ever leaves users' Devices. Consequently, Samsung does not and cannot access the Data, so Samsung does not possess or control it as those terms are understood in BIPA. Second, Samsung contends its facial scanning and resulting Data are not Biometrics because it cannot identify an individual. The Court reviews each argument in turn.

A. Whether Samsung Possessed Biometric Information under Section 15(a)

Section 15(a) only applies to private entities that are "in possession of" Biometrics. BIPA does not define "possession", so courts use its "popularly understood meaning." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186 ¶ 29, 432 Ill.Dec. 654, 129 N.E.3d 1197. "[P]ossession, as originally understood, occurs when a person has or takes control of the subject property or holds the property at his or her disposal." *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (quoting *People v. Ward*, 215 Ill.2d 317, 294 Ill.Dec. 144, 830 N.E.2d 556, 560 (2005)). In the context of BIPA, "possession occurs when someone exercises any form of control over the [biometric] data or held the data at his disposal." *Jacobs v. Hanwha Techwin America, Inc.*, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021) (quoting *Heard*, 440 F. Supp. 3d 960, at 968) (cleaned up).

***3** The parties' central disagreement is whether a private entity is in possession of Biometrics when it creates and controls technology that purportedly generates Biometrics, even if the entity does not receive or access the data.[5] [*Compare* Dkt. 55 at 11-12 ("Plaintiffs' conclusory allegations of Samsung's control over design decisions about

[the App] do not mean that Samsung 'possessed' data that is later generated and stored locally on Plaintiffs' devices while the devices are in Plaintiffs' possession"); *with* Dkt. 62 at 13 (Samsung is in possession of Plaintiffs' Biometrics because "Samsung has complete and total control over the biometric data surreptitiously captured using proprietary software that Samsung owned and alone controlled, preventing users from turning it off or disabling it").] There is caselaw that supports both parties' positions.

Plaintiffs liken their allegations to those in *Hazlitt. Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643 (S.D. Ill. 2021); [Dkt. 62 at 7.] Like here, *Hazlitt* involved a pre-installed, unmodifiable picture app that scanned and collected data from face geometries with the resulting data kept "locally in a facial recognition database in the solid-state memory on the device."[6] *Id.* at 646-47. Apple argued it did not possess Biometrics because "Plaintiffs have the choice to erase any or all data stored on their devices, only the plaintiffs know the identities of anyone in their photos, and there is no suggestion in the Complaint that Apple reserves the right to access a user's photos after selling the device." *Id.* at 652. The court sided with plaintiffs, holding they adequately alleged Apple possesses the data "because it has complete and exclusive control over the data on Apple Devices, including what biometric identifiers are collected, what biometric data is saved, whether biometric identifiers are used to identify users (creating biometric information), and how long biometric data is stored." *Id.* at 653.

Samsung's chief authority is *Barnett v. Apple Inc.*, 2022 IL App (1st) 220187, 469 Ill.Dec. 759, 225 N.E.3d 602, a case involving Apple's "Touch ID" and "Face ID" features. Also like this case, Apple developed and owned these technologies, and the resulting data was stored on the local user's device through mathematical representations. *Id.* ¶¶ 12, 14-15. Unlike this case, however, use of these features was voluntary, and users had the ability to delete the biometric information from their device. *Id.* ¶ 44. The *Barnett* court rejected plaintiff's argument that "Apple 'possess' their [biometric] information because Apple software collects and analyzes their information." *Id.* ¶ 43. The court reasoned this wrongfully "equates the product with the company" and that there is a salient difference between the data collected from a product created by the company, and the data the company itself possesses. *Id.; see also id.* ¶ 44 ("the device and the software are the tools, but it is the user herself who utilizes those tools to capture her own biometric information.")

***4** In so ruling, *Barnett* distinguished *Hazlitt* thus: "the plaintiffs in *Hazlitt* alleged that Apple stored the facial information in Apple's own databases and that users had no power to delete the collected information or disable the feature on their devices." *Id.* ¶ 45. Plaintiffs argue *Barnett*'s reference to "Apple's own databases" is the same database referred to in *Hazlitt*—the local database on the user's Device—so the sole difference between *Barnett* and *Hazlett* is that the consumer in *Barnett* had the option to use and/or remove her biometrics. [Dkt. 62 at 15-16.] Samsung posits *Barnett*'s holding is not about the amount of control a defendant (or plaintiff) has over the technology, but the defendant's level of access to the biometric data, which Apple had (at least to some degree) in *Hazlitt*.[7] [Dkt. 64 at 9.] And because Plaintiffs here have not alleged that Samsung has accessed or can access the Data (as opposed to the technology the App employs), Samsung is not in possession. [*Id.*]

The court in *Bhavilai* agreed with Samsung's logic. *Bhavilai v. Microsoft Corp.*, —— F. Supp. 3d ——, ——, 2024 WL 992928, at *1 (N.D. Ill. Feb. 8, 2024). In that case, the plaintiff alleged Microsoft was in possession of her biometric data, even though she admitted the data was not "physically stored on Microsoft's hardware", because a photo application Microsoft "owned and controlled" possessed her facial scan. *Id.* Plaintiff argued Microsoft was in possession of her biometric data "because it designed, licensed, and updated the facial scan software on users' devices" so Microsoft "exercised control over the device users' ability to access and use the facial scan software." *Id.* The Court rejected this argument and dismissed the plaintiff's Section 15(a) claim because the plaintiff failed to allege "Microsoft used or exercised any control over her facial scan data in any way." The Court added "the fact that Microsoft has the ability to give users the ability to collect facial scan data does not mean that Microsoft possesses the facial scan data." *Id.*

Other courts in this district have likewise found that control over the offending technology is insufficient; the defendant must have accessed or have access to the Biometrics. *Jacobs*, 2021 WL 3172967 (dismissing BIPA action against camera manufacturer with facial-recognition technology where manufacturer did not have access to camera footage or data used by third-party employer); *Heard*, 440 F. Supp. 3d 960, at 968 (plaintiff's allegations regarding possession inadequate where complaint "does not say whether BD could freely access the [biometric] data or even how BD allegedly received it.") Conversely, when the plaintiff alleges defendants possess the Biometrics, the Section 15(a)

claim proceeds. *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 284 (N.D. Ill. 2019) ("Namuwonge's allegation that Brookdale disclosed their employees' fingerprint data to Kronos sufficiently alleges that Kronos possessed the fingerprint data collected by Brookdale.")

The Court concludes Plaintiffs have not adequately alleged Samsung was "in possession" of their Biometrics. Samsung controls the App and its technology, but it does not follow that this control gives Samsung dominion over the Biometrics generated from the App, and plaintiffs have not alleged Samsung receives (or can receive) such data. Multiple courts have held these allegations are insufficient where the defendant does not also receive the underlying data:

> Bhavilai alleges that Microsoft exercised control over the device users' ability to access and use the facial scan software. But control of the facial scan software is not the same as control of the facial scan data that is collected using the software. Bhavilai has not alleged that Microsoft used or exercised any control over her facial scan data in any way. The fact that Microsoft has the ability to give users the ability to collect facial scan data does not mean that Microsoft possesses the facial scan data.

***5** *Bhavilai*, —— F. Supp. 3d at ——, 2024 WL 992928, at *1; *Barnett*, 2022 IL App (1st) 220187 ¶ 43, 469 Ill.Dec. 759, 225 N.E.3d 602 (the argument that a defendant possesses information because the software it owns "collects and analyzes their information ... equates the product with the company"); *see also Heard*, 440 F.Supp.3d 960, at 968 (no possession where plaintiff failed to allege defendant could access or receive the data).

The Court also disagrees that "possession" should turn on whether the technology is optional. Under BIPA, "possession does not contemplate [i.e., require] exclusive control", *Heard*, 440 F.Supp.3d 960, at 968, so Samsung would not lose possession because Plaintiffs also have it. Put differently, possession must be viewed from the eyes of the possessor, Samsung, which does not change if Plaintiffs have the option to alter settings in the App. Ultimately, the Court concludes the salient inquiry for determining possession under Section 15(a) is whether the entity exercised control over the Biometrics, not whether it exercised control over the technology generating the Biometrics. Plaintiffs have no allegations to that effect, so Samsung's motion to dismiss on this basis is granted.

B. Whether Samsung Collects, Captures, or Otherwise Obtains Biometrics under Section 15(b)

To state a Section 15(b) claim, a plaintiff must allege the defendant entity "collects", "captures", "or otherwise obtains" a person's Biometrics. 740 ILCS 14/15(b). As with "possession", BIPA does not provide definitions for these terms, so courts supply their "popularly understood meaning." *Rosenbach*, 2019 IL 123186 ¶ 29, 432 Ill.Dec. 654, 129 N.E.3d 1197. "Collect" means "to receive, gather, or exact from a number of persons or other sources", whereas "capture" means "to take, seize, or catch." *Cothron v. White Castle System, Inc.*, 2023 IL 128004 ¶ 23, 466 Ill.Dec. 85, 216 N.E.3d 918. Courts have understood "otherwise obtain" to mean procure through effort. *Heard*, 440 F. Supp. 3d 960, at 966; *Jones v. Microsoft Corp.*, 649 F. Supp. 3d 679, 683-84 (N.D. Ill. 2023). Collectively, all these verbs "mean to gain control" of Biometrics. *Cothron*, 2023 IL 128004 ¶ 16, 466 Ill.Dec. 85, 216 N.E.3d 918. This requires the defendant to make an affirmative effort—to take an "active step"—towards receiving the Biometrics. *Jones*, 649 F. Supp. 3d 679, at 683-84; *Heard*, 440 F. Supp. 3d 960, at 966; *Jacobs*, 2021 WL 3172967, at *2.

Plaintiffs contend Samsung has obtained their Biometrics through the App's collection of the Data. [Dkt. 62 at 19.] According to Plaintiffs, Samsung necessarily "obtained" the Data because otherwise the technology could not function—the App would have no ability to compare facial images. [*Id.* at 19-20.] Plaintiffs further argue Samsung took an "active step" by developing the App in a way that "automatically harvests biometric data from every photo stored on the Device and not only conceals this from users, but prevents them from disabling the process or destroying that information." [*Id.* at 20.] In essence, Plaintiffs' position is that the same conduct that caused Samsung to violate Section 15(a) makes it in violation of Section 15(b).

The Court disagrees. Plaintiffs' argument again conflates technology with Biometrics. But Section 15(b) is concerned with private entities collecting, capturing, or obtaining Biometrics, not creating technology. Plaintiffs do not allege Samsung receives the Data the App accumulates, or that

Samsung even has access to it. Indeed, Plaintiffs do not allege that Samsung takes any action towards the Data whatsoever after it is generated.

***6** This allegation is crucial to stating a Section 15(b) claim. In *Cothron*, for example, plaintiffs alleged White Castle affirmatively stored fingerprints on its own databases and used those fingerprints to give plaintiffs access to White Castle computers. These allegations satisfied Section 15(b) because this system could not function unless White Castle collected or captured the fingerprints. *Cothron*, 2023 IL 128004 at ¶ 23, 466 Ill.Dec. 85, 216 N.E.3d 918. Consistently, in *Heard*, the Court dismissed a Section 15(b) claim where the plaintiff failed to "allege how the data made its way to BD's systems." 440 F.Supp.3d 960, at 967. After an opportunity to amend, however, the Court permitted the Section 15(b) claim to proceed because plaintiffs now alleged BD "stores users' biometric information both on the device *and* in BD's servers." *Heard*, 524 F. Supp. 3d at 841 (emphasis in original). The Court further explained it was not BD's mere possession of Biometrics that satisfied 15(b)'s requirements, but that the allegations "suggest that BD itself plays an active role in collecting or otherwise obtaining users' biometric information." *Id.*

Here, Plaintiffs do not argue that Samsung possesses the Data or took any active steps to collect it. Rather, the active step according to Plaintiffs is the creation of the technology. This argument was flatly rejected in *Bhavilai*:

> Bhavilai argues that Microsoft 'collected' her facial scan data when it 'enabled the facial biometric scanning within its Photos application.' Bhavilai argues that because Microsoft retained the ability to control whether and how a user could use the facial scan software demonstrates that Microsoft was in fact the collector. But selling or licensing a tool that can be used to collect a facial scan is not the same as actually doing the collecting. This argument conflates two different activities—providing the tool versus using the tool. Bhavilai has simply failed to allege that Microsoft did anything beyond providing a tool.

Bhavilai, —— F. Supp. 3d at ——, 2024 WL 992928, at *1. As with Section 15(a), there is a salient difference between providing a technology and then using that technology to collect, capture, or obtain Biometrics. Here, Plaintiffs have failed to allege Samsung took an "active step" in gaining control over their Biometrics, which dooms their Section 15(b) claim.

C. Whether BIPA Regulates the App and its Data

Samsung raises an additional argument as to why Plaintiffs' claims fail: the App does not generate "biometric identifiers" or "biometric information" subject to BIPA's regulation. [Dkt. 55 at 16.] The Court agrees, which provides another basis for the dismissal of Plaintiffs' claims.

Plaintiffs argue the App's functions implicate BIPA in two ways. First, the App scans facial geometry, which is an explicitly enumerated biometric identifier. Second, the App's storage of Data (mathematical representations of face templates) constitutes biometric information. [Dkt. 62 at 25.] Samsung's posits that neither process can identify individuals; rather, they are only capable of recognizing faces, so BIPA does not apply. [Dkt. 55 at 17-18.]

As stated above, a "biometric identifier" "means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. Courts are divided on whether a plaintiff must allege a biometric identifier can identify a particular individual, or if it is sufficient to allege the defendant merely scanned, for example, the plaintiff's face or retina. *Compare e.g., Brown v. AS Beauty Group LLC*, 2024 WL 2319715 (N.D. Ill. May 22, 2024) (rejecting argument that biometric identifiers must be capable of identifying particular individuals); *Konow v. Brink's Inc.*, —— F.Supp.3d ——, ——, 2024 WL 942553, at *4 (N.D. Ill. Mar. 5, 2024) (requirement that biometric identifiers identify a unique person is not "supported by BIPA's plain language"); *Colombo v. YouTube, LLC*, 679 F. Supp. 3d 940 (N.D. Cal. 2023) (same); *with Martell v. X Corp.*, 2024 WL 3011353, at *3 (N.D. Ill. June 13, 2024) ("if the Court were to read BIPA as applying to any retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry without those items actually identifying an individual, it would contravene the very purpose of BIPA"); *Clarke v. Aveda Corp.*, —— F.Supp.3d ——, ——, 2023 WL 9119927, at *2 (N.D. Ill. Dec. 1, 2023) (dismissing BIPA complaint that "contains no plausible allegations that Aveda's collection of their biometric data made Aveda capable of determining their identities") (cleaned up); *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117, 1123 (9th Cir. 2024) ("scans of face geometry ... are not covered by BIPA if they cannot identify a person.")

***7** Central to this disagreement is what meaning, if any, should be given to the word "identifier" in "biometric identifier." *Compare Hazlitt v. Apple Inc.*, 500 F. Supp. 3d 738, 749 (S.D. Ill. 2020) ("Apple reads the word 'identifier' to exclude data that does not identify an actual person. This

Court finds that interpretation too narrow"); *with Zellmer*, 104 F. 4th 1117, at 1123 ("Zellmer would write the term 'identifier' out of BIPA. Under his reading, every 'retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry' is a biometric identifier and therefore within BIPA's reach. But this reading conflates necessary and sufficient conditions.") The parties' arguments fall along these exact lines; Plaintiffs urge the Court to conclude every scan is necessarily a biometric identifier, whereas Samsung argues the plain meaning of "identifier", combined with BIPA's purpose, demonstrates that only those scans that can identify an individual qualify. [Dkt. 55 at 17-18; Dkt. 62 at 25.] Samsung has the better argument.

Plaintiffs' position is grounded in a comparison of statutory definitions. Unlike the definitions of "biometric information" and "confidential and sensitive information", 740 ILCS 14/10, the term "biometric identifier" does not include language stating it must be capable of "identifying an individual." [Dkt. 62 at 24 ("[n]othing in the definition of "biometric identifier" requires any of those items to be used (or be capable of being used) to identify a person").]

While this distinction is accurate, that does not mean the word "identifier" should be ignored. *Mosby v. Ingalls Memorial Hospital*, 2023 IL 129081 ¶ 36, 473 Ill.Dec. 499, 234 N.E.3d 110 (when interpreting statutes in Illinois, "[e]ach word in a statute is to be 'given a reasonable meaning and not rendered superfluous' ") (quoting *Sylvester v. Industrial Comm'n*, 197 Ill.2d 225, 258 Ill.Dec. 548, 756 N.E. 2d 822, 827 (Ill. 2001)). "An 'identifier' is 'one that identifies,' and 'identify' means 'to ascertain the identity of [something or someone].' " *Zellmer*, 104 F. 4th 1117, at 1123 n.1; *see also Martell*, 2024 WL 3011353, at *3 ("Merriam-Webster defines 'identifier' as 'one that identifies' and Black's Law Dictionary defines 'identify' as 'to prove the identity of (a person or thing).' ")

Based on these principles of statutory interpretation and the plain meaning of identifier, the Court concludes BIPA only covers those "retina or iris scan[s], fingerprint[s], voiceprint[s], or scan[s] of hand or face geometry" that are capable of identifying an individual. Therefore, the fact that the App performs face scans is not dispositive.

This holding comports with the legislation's intent in enacting BIPA. *Sylvester*, 258 Ill.Dec. 548, 756 N.E. 2d 822, at 827 (in matters of statutory construction, the "primary goal, to which all other rules are subordinate, is to ascertain and give effect to the intention of the legislature.") BIPA recognizes that biometrics "are biologically unique to the individual [and] once compromised, the individual has no recourse." 740 ILCS 14/5(c). For biometrics to be compromised, however, there must be some ability to connect the biometrics to an individual; a facial scan is meaningless if there is no way to determine who it belongs to. That is why the terms "biometric information" and "confidential and sensitive information" make clear the information must be capable of identifying the individual. But as the Ninth Circuit reasoned, it was unnecessary to add this language to biometric identifier because it is baked into the term. *Zellmer*, 104 F.4th 1117, at 1124 ("the ability to identify did not need to be spelled out in that term—it was readily apparent from the use of 'identifier.' ")

The Court now turns to whether any function within the App is capable of identifying an individual. Again, the parties disagree on what level of identification is required. Plaintiffs contend the App's creation of unique mathematical representations of a person's face is sufficient because the technology identifies and groups unique faces. [Dkt. 62 at 25-26 ("Samsung uses the Face Templates to recognize the person among the sea of faces appearing on the hundreds (if not thousands) of photographs stored in the Gallery App").]

***8** According to Plaintiffs, it does not matter that the App cannot—either through the creation of the face template or in combination with other information on the Device—ascertain an individual's identity, [*id.* at 26], which is Samsung's argument. [Dkt. 55 at 18 (the Data cannot "identify who the individuals in the photos are. To the contrary: users' own knowledge, not the technology, is what may identify people in their photographs").]

Although this is another issue with law on both sides, the Court follows the line of cases that require biometric information to be capable of recognizing an individual's identity, not simply an individual's feature. *Zellmer*, 104 F. 4th 1117, at 1125 (holding that technology that cannot identify individuals does not fall within BIPA); *Castelaz v. Estee Lauder Companies, Inc.*, 2024 WL 136872, at *6-7 (N.D. Ill. Jan. 10, 2024) (dismissing BIPA claim where plaintiffs failed to provide "any specific factual allegations that [defendant] is capable of determining Plaintiffs and members of the Illinois class members' identities by using the collected facial scans, whether alone or in conjunction with other methods or sources of information available to" defendant); *Clarke*, —— F.Supp.3d ——, 2023 WL 9119927 (same).

The *Daichendt* cases provide a helpful example. In ruling on a motion to dismiss the initial complaint, the district court held that for a BIPA claim to survive, "plaintiffs must allege that defendant's collection of their biometric data made defendant *capable of* determining their identities." *Daichendt v. CVS Pharmacy, Inc.*, 2022 WL 17404488, at *5 (N.D. Ill. Dec. 2, 2022) (emphasis in original). The court held plaintiffs failed to meet this burden because they did not allege CVS had any way, "such as their names or physical or email addresses, that could connect the voluntary scans of face geometry with their identities." *Id.* Accordingly, plaintiffs "failed to plead the most foundational aspect of a BIPA claim"—the ability to identify an individual—and their claim was dismissed. *Id.* In the amended complaint, however, plaintiffs alleged they included "their names, email addresses, and phone numbers into a computer terminal inside defendant's stores prior to scanning their biometric identifiers", which was sufficient to survive the motion to dismiss. *Daichendt v. CVS Pharmacy, Inc.*, 2023 WL 3559669, at *1 (N.D. Ill. May 4, 2023).

In arguing that individual identification is not a statutory requirement, Plaintiffs cite to several cases. But all these cases included allegations regarding a combination of factors that allowed individual identification. *Rosenbach*, 2019 IL 123186, 432 Ill.Dec. 654, 129 N.E.3d 1197 (thumbprint scan in combination with personal identifying information); *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 517 (N.D. Ill. 2022) (AI technology that could "actually identify unique individuals"); *Hazlitt*, 500 F. Supp. 3d 738, at 749 (photography app that "applies an algorithm to identify the device user"); *Rivera v. Google*, 238 F.Supp.3d 1088, 1095 (N.D. Ill. 2017) (photography app that is capable of identifying a specific person).

Here, Plaintiffs do not allege the App's technology is capable of identifying a person's identity. Rather, Plaintiffs allege only that the App groups unidentified faces together, and it is the Device user who (has the option to) add names to the faces. The Court concludes these allegations are insufficient to show that the Data constitutes either a biometric identifier or biometric information.

IV. Conclusion

***9** For these reasons, Samsung's motion to dismiss is granted. The dismissal will be without prejudice. Although Plaintiff G.T. has already had an opportunity to amend the complaint once, [Dkts. 1, 14], the operative pleading came before the motion to dismiss was filed. The Court's normal practice, in accordance with Seventh Circuit guidance, is to give one chance to amend after a motion to dismiss is briefed, even if a plaintiff has amended previously. *Zimmerman v. Bornick*, 25 F.4th 491, 494 (7th Cir. 2022). And Seventh Circuit precedent is clear that the Court should err on the side of allowing an amendment; "a court should deny leave to amend only if it is certain that amendment would be futile or otherwise unwarranted." *Runnion ex rel. Runnion v. Girl Scouts of Greater Chi. & Nw. Ind.*, 786 F.3d 510, 520 (7th Cir. 2015). While there is some doubt on these facts, it is not certain that "any amendment would be futile." *Id.*

All Citations

--- F.Supp.3d ----, 2024 WL 3520026

Footnotes

1 Plaintiffs are G.T., by and through next friend Liliana T. Hanlon, Shimera Jones, Leroy Jacobs, Richard Maday, Mark Heil, Balarie Cosby-Steele, Sherie Harris, John DeMatteo, and Allison Thurman. The Court will refer to them collectively as "Plaintiffs."

2 Citations to docket filings generally refer to the electronic pagination provided by CM/ECF, which may not be consistent with page numbers in the underlying documents.

3 Facial geometry includes various measurements such as the length between the eyes, as well as the shape, width and depth of the mouth, chin, nose, ears, eyebrows, etc.

4 The Court will refer to these terms collectively as "Biometrics."

5 Plaintiffs make two arguments that Samsung received the Data. Both are unavailing. Plaintiffs allege the App had "a feature that allow[ed] users to backup their photographs to a [centralized] cloud server" until September 2021, but photographs are explicitly excluded from the definition of biometric identifiers, and Plaintiffs do not allege the underlying Data was uploaded to the cloud. [*See* Dkt. 62 at 10-11; Dkt. 50 ¶ 66.] Second, Plaintiffs allege in several places that the Data is "at least" stored on the local Device (keeping open the possibility that Samsung received the Data elsewhere) but that is impermissibly speculative; Plaintiffs must allege facts. *Cochran*, 828 F.3d 597, at 599.

6 The *Hazlitt* court noted Apple "does not store or transfer all user biometric identifiers or biometric information on its servers", which suggests at least some Biometrics were sent to Apple. *Id.* at 647.

7 After discovery was taken in *Hazlitt*, plaintiffs filed an amended complaint alleging the biometric information was sent to Apple's centralized servers. *Doe v. Apple Inc.*, 2022 WL 17538446, at *1 (S.D. Ill. Aug. 1, 2022).

End of Document

EXHIBIT 3

2024 WL 3011353
Only the Westlaw citation is currently available.
United States District Court, N.D. Illinois, Eastern Division.

Mark MARTELL, on behalf of himself and all others similarly situated, Plaintiff,
v.
X CORP., Defendant.

Case No. 23 C 5449
|
Signed June 13, 2024

Attorneys and Law Firms

Carl V. Malmstrom, Wolf Haldenstein Adler Freeman & Herz LLC, Chicago, IL, Joseph I. Marchese, Pro Hac Vice, Philip L. Fraietta, Pro Hac Vice, Bursor & Fisher P.A., New York, NY, for Plaintiff.

Robert Collins, III, Kathryn Running, Latham & Watkins LLP, Chicago, IL, for Defendant.

MEMORANDUM OPINION AND ORDER

Sunil R. Harjani, United States District Judge

***1** In this lawsuit, Plaintiff Mark Martell brings a Class Action Complaint on behalf of himself and others similarly situated for violations of the Illinois Biometric Information Privacy Act (BIPA) against Defendant X Corp.[1] Martell alleges that he uploaded a photograph of himself on the social media platform X (formerly known as Twitter), which X analyzed for nudity and other not-safe-for-work content using a Microsoft product called PhotoDNA. Plaintiff alleges that PhotoDNA created a unique digital signature of the photograph, known as a "hash", to compare against other photographs' hashes. As a result, Plaintiff alleges that creating this hash necessarily created a scan of his facial geometry in violation of BIPA. Defendant moved to dismiss the Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6), claiming that the Complaint fails to state a claim upon which relief can be granted. For the reasons stated below, Defendant's motion [15] is granted.

Legal Standard

"A motion under Rule 12(b)(6) tests whether the complaint states a claim on which relief may be granted." *Richards v. Mitcheff*, 696 F.3d 635, 637 (7th Cir. 2012). To survive a Rule 12(b)(6) motion, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). This pleading standard does not necessarily require a complaint to contain detailed factual allegations. *Twombly*, 550 U.S. at 555. Rather, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Adams v. City of Indianapolis*, 742 F.3d 720, 728 (7th Cir. 2014) (quoting *Iqbal*, 556 U.S. at 678). When deciding a motion to dismiss under Rule 12(b)(6), the court accepts as true all factual allegations in the complaint and draws all inferences in favor of the plaintiff. *Heredia v. Capital Management Services, L.P.*, 942 F.3d 811, 814 (7th Cir. 2019). However, a complaint must consist of more than "threadbare recitals of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 555).

Discussion

The Defendant raises three primary issues with the Complaint. First, Defendant argues the Complaint should be dismissed because Plaintiff fails to plausibly allege that PhotoDNA collects facial geometry scans as defined by BIPA. Second, Defendant contends that the hashes created by PhotoDNA are not biometric information or biometric identifiers under BIPA because they cannot be used to identify a person. Finally, Defendant argues that the Communication Decency Act bars Plaintiff's claim.[2] The Court will address each of these arguments in turn.

***2** Initially, it is important to understand what BIPA protects. In 2008, the Illinois legislature found that businesses were increasingly using biometrics to streamline financial transactions and security screenings. The legislature found that biometrics—unlike other identifiers such as social security numbers that can be changed if compromised—are "biologically unique to the individual; therefore, once

compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c). The legislature also found that an overwhelming majority of the public was weary of using biometrics when such information was tied to finances and other personal information. Since the full ramifications of biometric technology were not fully known, the legislature found that "public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g).

BIPA prohibits private entities from collecting or capturing "a person's or a customer's biometric identifier or biometric information" without first providing written notice that the information is being collected and of the specific purpose and length of the term for the collection, storage, and use of the data. 740 ILCS 14/15(b). The entity must then receive written consent from the subject of the biometric identifier or biometric information. *Id.* BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. BIPA further defines "biometric information" as any information "based on an individual's biometric identifier used to identify an individual." *Id.*

Facial Geometry

Defendant first argues that the Complaint should be dismissed because Plaintiff fails to plausibly allege that PhotoDNA collects facial geometry scans as defined by BIPA. Defendant contends that according to Microsoft's website, which Plaintiff cited in the Complaint, PhotoDNA is not facial recognition software and cannot be used to identify a person, so it cannot be a scan of facial geometry. Defendant argues that an allegation that PhotoDNA scanned the facial geometry of the individuals in the photograph is required for the scans to be considered a biometric under BIPA. Plaintiff responds that he sufficiently alleged that PhotoDNA scans for facial geometry.

Whether PhotoDNA scans for facial geometry is an important consideration because a scan of face geometry is required for the conduct to be covered by BIPA. BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. The statute then goes on to list items that do not qualify as biometric identifiers including writing samples, written signatures, demographic data, tattoo descriptions, physical descriptions, and relevant to this dispute, photographs. *Id.* Thus, Plaintiff must allege that the PhotoDNA scanned individuals' face geometry and not just that it scanned a photo. This consideration also impacts what qualifies as biometric information because biometric information is "based on an individual's biometric identifier," so if PhotoDNA only scans a photograph, it is not biometric information.

Plaintiff responds that he sufficiently alleged that the PhotoDNA software collected facial geometry scans when it created the unique hash for the photograph. Specifically, Plaintiff alleged that "PhotoDNA creates a unique digital signature (known as a 'hash') of an image which is then compared against signatures (hashes) of other photos to find copies of the same image." Compl. [1-2] ¶ 25. Plaintiff included in the Complaint an image from Microsoft's website, which he alleged shows that PhotoDNA creates "a unique digital signature, or 'hash,' from any image containing a person's face [which] necessitates creating a scan of that person's facial geometry." *Id.* ¶ 27. The Court finds that these allegations are conclusory. The fact that PhotoDNA creates a unique hash for each photo does not necessarily imply that it is scanning for an individual's facial geometry when creating the hash.

***3** The absence of factual allegations to this point is evident when Plaintiff's allegations are compared to BIPA complaints where district courts found that a plaintiff plausibly alleged that the defendant collected their biometric identifier. For example, in *Carpenter v. McDonald's Corp.*, the plaintiff alleged that the defendant's "AI voice assistant is able to extract voice information including pitch, volume, and duration along with identifying information like age, gender, nationality, and national origin." 580 F. Supp. 3d 512, 517 (N.D. Ill. 2022). The plaintiff also alleged that the AI voice assistant used an acoustic model that was trained to receive "a graphical representation, measurement, or illustration of acoustic patterns." *Id.* The court also noted that "importantly, Plaintiff alleges that McDonald's uses the AI and data to actually identify unique individuals." *Id.* The court found that these allegations were sufficient to plausibly allege that the technology "mechanically analyzes customers' voices in a measurable way such that McDonald's has collected a voiceprint[.]" *Id.* Here, Plaintiff has not made similar factual allegations but instead merely concludes that creating the digital hash "necessitates creating a scan of that person's facial

geometry." Compl. [1-2] ¶ 27. Plaintiff's Complaint does not include factual allegations about the hashes including that it conducts a face geometry scan of individuals in the photo. Allegations that a photo was scanned are insufficient to plausibly allege that PhotoDNA creates a scan of an individual's face geometry under BIPA.

Similarly, in *Rivera v. Google Inc.*, the plaintiff alleged that when she was photographed on a Google Android device, those photos were automatically uploaded to Google Photos and Google immediately scanned each of the photos. 238 F. Supp. 3d 1088, 1091 (N.D. Ill. 2017). The plaintiff alleged that the scans "located her face and zeroed in on its unique contours to create a 'template' that maps and records her distinct facial measurements." *Id.* The court found that the allegation that Google created a biology-based face template of the individuals in the photos was sufficient to allege a scan of face geometry under BIPA. *Id.* at 1095. Importantly, the court noted that the plaintiff was not alleging that the photos themselves were biometric identifiers, but rather that the face templates were biometric identifiers. *Id.* at 1096. Here, Plaintiff has not made that distinction. While Plaintiff alleged that PhotoDNA scanned the photo to create a unique hash, Plaintiff did not allege facts indicating that the hash is a scan of face geometry, as opposed to merely a record of the photo. Plaintiff's allegations leave open the question of whether the hash is a unique representation of the entire photo or specific to the faces of the people in the picture. If the scan merely compares the image to see if it is the same as other images, that does not imply the use of facial geometry. If, instead, PhotoDNA identifies and scans the facial geometry of individuals in the photos and the hash saves those facial geometry scans, then it could be a biometric identifier under BIPA. But Plaintiff does not allege that the hash process takes a scan of face geometry, rather he summarily concludes that it must. The Court cannot accept such conclusions as facts adequate to state a plausible claim.

Biometric Identifiers and Biometric Information

Defendant next argues that Plaintiff failed to allege a viable BIPA claim because the Complaint does not allege that PhotoDNA could be used to identify the individuals in the photos. Defendant argues that biometric information must be used to identify an individual because, as defined by the statute, BIPA biometric information is any information "based on an individual's biometric identifier *used to identify an individual*." 740 ILCS 14/10 (emphasis added). Plaintiff does not dispute that this is required under the definition of biometric information and instead argues that the PhotoDNA hashes qualify as "biometric identifiers" and further that BIPA does not require that biometric identifiers be used to identify an individual because, unlike the definition for biometric information, the definition for biometric identifier does not include the 'used to identify an individual' language.

While Plaintiff is correct that the definition of biometric identifier does not include the phrase 'used to identify an individual,' the term itself includes the word identifier. As defined by BIPA " 'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. When analyzing the plain language of the statute, a court in this district found that this was a specific and complete list where each item was "a biology-based set of measurements ('biometric') that can be used to identify a person ('identifier')." *Rivera*, 238 F. Supp. 3d at 1094. Further, Merriam-Webster defines "identifier" as "one that identifies" and Black's Law Dictionary defines "identify" as "to prove the identity of (a person or thing)." Merriam-Webster's Unabridged Dictionary; Black's Law Dictionary (11th ed. 2019). Beyond that, if the Court were to read BIPA as applying to any retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry without those items actually identifying an individual, it would contravene the very purpose of BIPA. If a face geometry scan could not identify an individual, how could a business provide the individual with notice and obtain their consent? BIPA requires that before a private entity can collect "a person's or a customer's biometric identifier," it must inform "the subject" that the information is being collected and receive "a written release executed by the subject of the biometric identifier[.]" 740 ILCS 14/15. Thus, under a plain reading of BIPA, Plaintiff must allege that the biometric identifier can be used to identify an individual.

***4** Plaintiff points to cases where courts found that other kinds of technology that scanned an individual's face geometry were a biometric identifier and argues that BIPA does not require him to allege that biometric identifiers are used to identify an individual. For example, Plaintiff relies on *Sosa v. Onfido, Inc.*, to support his argument that the hashes should be considered biometric identifiers. 600 F. Supp. 3d 859 (N.D. Ill. 2022). In *Sosa*, the plaintiff alleged that after defendant's software scans an individual's identification and photograph to locate the facial image in each document, it

extracts a "faceprint"—a unique numerical representation of the shape or geometry of each facial image—which it then compares to the consumer's identification and photograph, after which it generates a score based on the similarity of the faceprints. *Id.* at 865. The court found that as alleged, the software "scans identification cards and photographs to locate facial images and extracts a unique numerical representation of the shape or geometry of each facial image" which plausibly constituted a scan of face geometry. *Id.* at 871. Plaintiff has made no such allegations about PhotoDNA scanning the faces in photos uploaded on Twitter. Plaintiff only alleges that the photo was scanned, without alleging that the faces in the photo were scanned to identify an individual. Without allegations that PhotoDNA uses facial geometry to identify individuals, Plaintiff failed to allege that the hashes are biometric identifiers.

Plaintiff further relies on *American Civil Liberties Union v. Clearview AI, Inc.*, to support his argument that PhotoDNA's hashes should be considered facial scans. 2021 WL 4164452 (Ill. Cir. Ct. Aug. 27, 2021). However, as with *Sosa*, the allegations in *Clearview* are distinguishable from the facts Plaintiff alleges in the Complaint. In *Clearview*, when the system scanned a photo, it measured and recorded data such as the shape of the cheekbones and the distance between eyes, nose, and ears, and assigned that data a numerical value, which it then used to identify someone in other photos. *Id.* at *1. The court held that BIPA applied to such faceprints. *Id.* at *5. Here, Plaintiff does not allege that any details of an individual's face are measured or recorded during the PhotoDNA scan or that those records were used to identify individuals.

The fatal flaw in Plaintiff's Complaint is that he failed to allege that any type of facial scan occurs during the hash creation process. Without that, there can be no scan of face geometry which could be used to identify an individual, as is required to be considered a biometric identifier under BIPA. True, the cases Plaintiff cites all stand for the proposition that BIPA allows for face geometry scans to be created from photographs. *Sosa*, 600 F. Supp. 3d at 873 ("In conclusion, we join the Illinois courts that have uniformly rejected the argument that BIPA exempts biometric data extracted from photographs.") (internal citation and quotation omitted); *Clearview*, 2021 WL 4164452, at *5 (rejecting the argument that BIPA does not apply to faceprints derived from photographs).[3] But that principle alone does not save his Complaint because it fails to sufficiently allege that the PhotoDNA hashes consist of a scan of face geometry that could be used to identify an individual. Contrary to Plaintiff's arguments, courts have routinely held that a biometric identifier is "a biology-based set of measurements ('biometric') that can be used to identify a person ('identifier')." *Rivera*, 238 F. Supp. 3d at 1094.[4] As such, Plaintiff fails to sufficiently allege a BIPA claim and the Complaint is dismissed.

The Communication Decency Act

***5** Since the Court will provide Plaintiff with leave to file an amended complaint (if possible), the Court will address now Defendant's argument that the Communication Decency Act (CDA) preempts Plaintiff's claim. Defendant argues that its conduct was an effort to identify and remove child-exploitation and objectionable material from Twitter and as such falls within the preemptive scope of Section 230(c)(2)(A) of the CDA. Plaintiff contends that nothing in the Complaint alleged that Defendant's actions fall under the scope of the CDA and that since it is an affirmative defense, the Court should not grant the motion unless the Complaint pleads every element of the defense.

The CDA Section 230(c)(2) provides:

> No provider or user of an interactive computer service shall be held liable on account of—
>
> > (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected;

47 U.S.C. § 230(c)(2). Section 230 preempts causes of action and liability that "may be imposed under any State or local law that is inconsistent with this section." *Id.* § 230(e)(3).

At the outset, Defendant cited no case law where a court held the CDA preempted a BIPA claim and the Court found none. Defendant further asserts that it is entitled to immunity under § 230(c)(2)(A) because it is a provider of an interactive computer service that acted voluntarily in good faith to restrict

access to explicit images. Immunity under § 230(c)(2) is an affirmative defense so the Defendant bears the burden of proof. As CDA immunity frequently turns on facts not before the court at the pleading stage, dismissal is only appropriate when a plaintiff pleads themselves out of court. *Bonilla v. Ancestry.com Operations Inc.*, 574 F. Supp. 3d 582, 592 (N.D. Ill. 2021); *see Hyson USA, Inc. v. Hyson 2U, Ltd.*, 821 F.3d 935, 939 (7th Cir. 2016). Here, Plaintiff has not pled himself out of court. Taking the allegations in the light most favorable to Plaintiff, the Complaint does not allege that X acted in good faith, as required for immunity under § 230(c)(2). As such, Defendant is not entitled to immunity at this time.

Conclusion

For the reasons stated above, Defendant's motion to dismiss [15] is granted. Plaintiff may refile an amended complaint if he can cure the deficiencies and such an amendment is consistent with his obligations under Federal Rule of Civil Procedure 11. *Runnion ex rel. Runnion v. Girl Scouts of Greater Chicago & Nw. Indiana*, 786 F.3d 510, 519–20 (7th Cir. 2015) ("Unless it is certain from the face of the complaint that any amendment would be futile or otherwise unwarranted, the district court should grant leave to amend after granting a motion to dismiss."). If Plaintiff does not file an amended complaint by June 27, 2024, then the dismissal will automatically convert to a dismissal with prejudice.

SO ORDERED.

All Citations

Slip Copy, 2024 WL 3011353

Footnotes

1 Defendant X Corp. is the successor organization to Twitter, Inc.

2 In the alternative, Defendant argues that the Court should dismiss Plaintiff's Section 15(d) claim and his claim for enhanced statutory damages. The Court does not reach these arguments, because the Complaint was dismissed on other grounds.

3 *See, e.g.*, *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *3–5 (N.D. Ill. Sept. 15, 2017) (rejecting Shutterfly's arguments that a scan of face geometry cannot be done on photographs); *Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1296 (W.D. Wash. 2021) (finding that facial scans taken from photographs are biometric identifiers because they are "a set of measurements of a specified physical component ... used to identify a person."). Further, as the Defendant notes, it is undisputed that a facial geometry scan can be derived from a photograph and considered a biometric identifier under BIPA. *See* Doc. [19] at 4.

4 *See, e.g.*, *Sosa*, 600 F. Supp. 3d at 873 ("items identified as 'biometric identifiers' are 'specific, biology-based measurements used to identify a person, without reference to how the measurements were taken[.]' "); *Vance*, 525 F. Supp. 3d at 1296 ("The bottom line is that a 'biometric identifier' is ... a set of measurements of a specified physical component ... used to identify a person.").